

# Quantum Error Correction for Communication

Artur Ekert and Chiara Macchiavello  
Clarendon Laboratory, University of Oxford

February 1996

## Abstract

We show how procedures which can correct phase and amplitude errors can be directly applied to correct errors due to quantum entanglement. We specify general criteria for quantum error correction, introduce quantum versions of the Hamming and the Gilbert-Varshamov bounds and comment on the practical implementations of quantum codes.

Suppose we want to transmit a block of  $l$  qubits (i.e. two-state quantum systems) in some unknown quantum state (pure or mixed) over a noisy quantum channel. Here ‘noisy’ means that each transmitted qubit may, with some small probability  $p$ , become entangled with the channel. In order to increase the probability of the error-free transmission we can encode the state of  $l$  qubits into a set of  $n$  qubits and try to disentangle a certain number of qubits from the channel at the receiving end. This paper specifies conditions under which such encoding and disentanglement are possible.

Let us start with introducing convenient definitions and notation. Amplitude errors in a block of  $n$  qubits are defined as a sequence of  $\sigma_x$  transformations performed on qubits at locations specified by a binary  $n$ -tuple  $\alpha$  (non-zero entries of  $\alpha$  mark the locations of the affected qubits). In a selected basis  $\{v\}$  the amplitude errors can be written as

$$A_\alpha |v\rangle = |v + \alpha\rangle, \quad (1)$$

where the addition is performed modulo 2. Analogously, phase errors are defined as a sequence of  $\sigma_z$  transformations performed on qubits at locations

specified by a binary  $n$ -tuple  $\beta$  and can be written as

$$P_\beta |v\rangle = (-1)^{\beta \cdot v} |v\rangle, \quad (2)$$

where the addition in the scalar product  $\beta \cdot v$  is also performed modulo 2. For example, if  $\alpha = \beta = (001010)$  and  $v = (110111)$ , then

$$A_\alpha |110111\rangle = |111101\rangle, \quad P_\beta |110111\rangle = (-1) |110111\rangle. \quad (3)$$

Amplitude and phase errors are generated by unitary operations and are, of course, different from errors due to the qubit-channel entanglement, however, codes which can correct both amplitude and phase errors can also correct the entanglement induced errors. To illustrate the basic idea we start with a simple example of decoherence induced errors which can be rectified by phase correction alone. Consider the following scenario: we want to transmit one qubit in an unknown quantum state of the form  $c_0 |0\rangle + c_1 |1\rangle$  and we know that any single qubit which is transmitted via the channel can, with a small probability  $p$ , undergo a decoherence type entanglement with the channel

$$(c_0|0\rangle + c_1|1\rangle)|a\rangle \longrightarrow c_0|0\rangle|a_0\rangle + c_1|1\rangle|a_1\rangle, \quad (4)$$

where states  $|a\rangle, |a_0\rangle, |a_1\rangle$  are the states of the environment/channel and  $|a_0\rangle, |a_1\rangle$  are usually not orthogonal ( $\langle a_0|a_1\rangle \neq 0$ ). It turns out that with a simple encoding and phase error correcting procedure the probability of error can be reduced to be of the order  $p^2$ . To achieve this the sender can add two qubits, initially both in state  $|0\rangle$ , to the original qubit and then perform an encoding unitary transformation

$$|000\rangle \longrightarrow |C^0\rangle = |000\rangle + |011\rangle + |101\rangle + |110\rangle, \quad (5)$$

$$|100\rangle \longrightarrow |C^1\rangle = |111\rangle + |100\rangle + |010\rangle + |001\rangle, \quad (6)$$

(here and in the following we omit the normalisation factors) generating state  $c_0 |C^0\rangle + c_1 |C^1\rangle$ . Now, suppose that only the first transmitted qubit became entangled with the channel; the code-vectors  $|C^0\rangle$  and  $|C^1\rangle$  evolve as

$$|C^0\rangle |a\rangle \longrightarrow (|000\rangle + |011\rangle) |a_0\rangle + (|101\rangle + |110\rangle) |a_1\rangle \quad (7)$$

$$|C^1\rangle |a\rangle \longrightarrow (|111\rangle + |100\rangle) |a_1\rangle + (|010\rangle + |001\rangle) |a_0\rangle \quad (8)$$

The receiver applies two projection operators to the received triple of qubits. Projector  $L_1$  projects on the subspace spanned by  $\{|C^0\rangle, |C^1\rangle, P_{100}|C^0\rangle, P_{100}|C^1\rangle\}$  and  $L_2$  on the subspace spanned by  $\{|C^0\rangle, |C^1\rangle, P_{010}|C^0\rangle, P_{010}|C^1\rangle\}$ . If a state vector is projected on a specified subspace we say that the result of the projection is 1 and if the vector is projected on an orthogonal subspace we call the result 0. There are four possible results of the two subsequent projections  $L_1$  and  $L_2$ : when the result is 11 the final state is the original state  $c_0|C^0\rangle + c_1|C^1\rangle$ ; results 01, 10 and 00 correspond to final states which are related to the original one respectively via  $P_{100}$ ,  $P_{010}$ , and  $P_{001}$ . Depending on the result of the projections we apply one of these three phase correcting unitary operations and restore the state. This way we can achieve an error-free communication in cases when one qubit has decohered and as the result the probability of the successful transmission increases to  $1 - (1-p)^3 - 3(1-p)^2p \approx 1 - p^2$ . The reason why in this particular case the phase error correction (i.e. projections on subspaces of the form  $P_\beta|C^k\rangle$ ) can rectify errors due to decoherence is because the decoherence process described by Eq.(4) is mathematically equivalent to randomizing phase  $\phi$  in  $c_0|0\rangle + c_1e^{i\phi}|1\rangle$  [1].

Let us now consider the most general dissipation in the channel; each qubit can undergo the following entanglement

$$|0\rangle|a\rangle \longrightarrow |0\rangle|a_{0,0}\rangle + |1\rangle|a_{0,1}\rangle \quad (9)$$

$$|1\rangle|a\rangle \longrightarrow |0\rangle|a_{1,0}\rangle + |1\rangle|a_{1,1}\rangle. \quad (10)$$

The states of the channel/environment that entangle with the transmitted qubits are, in general, different for different qubits.

We will show now that in order to disentangle up to  $t$  qubits from the channel we need only amplitude and phase correction codes.

Codes which correct up to  $t$  amplitude errors are constructed by selecting  $2^l$  mutually orthogonal code-vectors  $|C^k\rangle$  ( $k = 1, 2, \dots, 2^l$ ) from the  $2^n$  dimensional state space of the  $n$  qubits such that

$$\langle C^k | A_\alpha A_{\alpha'} | C^l \rangle = \delta_{kl} \delta_{\alpha\alpha'}, \quad (11)$$

for any  $\alpha$  and  $\alpha'$  which satisfy  $\text{wt}(\alpha), \text{wt}(\alpha') \leq t$ , where  $\text{wt}(x)$ , the weight of  $x$ , is the number of values different from 0 in the  $n$ -tuple  $x$ . Projections on subspaces  $H_\alpha$  spanned by vectors  $\{A_\alpha|C^k\rangle; k = 1, 2, \dots, 2^l\}$  identify the error locations  $\bar{\alpha}$ , and the correcting operation  $A_{\bar{\alpha}}$  can be applied.

Codes which correct up to  $t$  phase errors are constructed by selecting  $2^l$  mutually orthogonal code-vectors  $|C^k\rangle$  ( $k = 1, 2, \dots, 2^l$ ) from the  $2^n$  dimensional state space of the  $n$  qubits such that

$$\langle C^k | P_\beta P_{\beta'} | C^l \rangle = \delta_{kl} \delta_{\beta\beta'}, \quad (12)$$

for any  $\beta$  and  $\beta'$  which satisfy  $\text{wt}(\beta), \text{wt}(\beta') \leq t$ . Projections on subspaces  $H_\beta$  spanned by vectors  $\{P_\beta | C^k\rangle; k = 1, 2, \dots, 2^l\}$  identify the error locations  $\bar{\beta}$ , and the correcting operation  $P_{\bar{\beta}}$  can be applied.

In order to correct the entanglement induced errors we will require that the code-vectors  $|C^k\rangle$  are carefully selected to satisfy the following condition

$$\langle C^k | P_\beta A_\alpha A_{\alpha'} P_{\beta'} | C^l \rangle = \delta_{kl} \delta_{\alpha\alpha'} \delta_{\beta\beta'}, \quad (13)$$

for all  $\alpha$  and  $\beta$  such that  $\text{wt}(\text{supp}[\alpha] \cup \text{supp}[\beta]) \leq t$  ( $\text{supp}[x]$  denotes the set of locations where the  $n$ -tuple  $x$  is different from zero). Both conditions (11) and (12) are particular cases of (13). The encoding unitary transformation maps the basis states of the original  $2^l$ -dimensional Hilbert space into  $2^l$  states  $\{|C^k\rangle\}$  in the enlarged  $2^n$ -dimensional Hilbert space. To see how the two codes can disentangle up to  $t$  qubits from the channel consider a particular case when  $t = 2$  (cases  $t > 2$  can be proved by a simple extension of the argument presented below).

Let us denote by  $| (00) \rangle$  a subset (or a superposition) of the basis states in which the two qubits affected by the dissipation process described by Eqs.(9)-(10) are initially both in state  $|0\rangle$ , and analogously for  $| (01) \rangle$ ,  $| (10) \rangle$  and  $| (11) \rangle$ . For simplicity, let us now restrict our attention to one of the code-vectors  $\{|C^k\rangle\}$ , it can be written as

$$|C^k\rangle = | (00) \rangle_1^k + | (01) \rangle_2^k + | (10) \rangle_3^k + | (11) \rangle_4^k. \quad (14)$$

After the dissipation the state  $|C^k\rangle |a\rangle$  has the form

$$\begin{aligned} & | (00) \rangle_1^k |a_{00,00}\rangle + | (01) \rangle_2^k |a_{01,01}\rangle + | (10) \rangle_3^k |a_{10,10}\rangle + | (11) \rangle_4^k |a_{11,11}\rangle + \\ & | (01) \rangle_1^k |a_{00,01}\rangle + | (00) \rangle_2^k |a_{01,00}\rangle + | (11) \rangle_3^k |a_{10,11}\rangle + | (10) \rangle_4^k |a_{11,10}\rangle + \\ & | (10) \rangle_1^k |a_{00,10}\rangle + | (11) \rangle_2^k |a_{01,11}\rangle + | (00) \rangle_3^k |a_{10,00}\rangle + | (01) \rangle_4^k |a_{11,01}\rangle + \\ & | (11) \rangle_1^k |a_{00,11}\rangle + | (10) \rangle_2^k |a_{01,10}\rangle + | (01) \rangle_3^k |a_{10,01}\rangle + | (00) \rangle_4^k |a_{11,00}\rangle. \end{aligned} \quad (15)$$

By expressing each component of (14) as a linear combination of phase projectors acting on  $|C^k\rangle$ :

$$|(00)\rangle_1^k = (1 + P_{01} + P_{10} + P_{11})|C^k\rangle \quad (16)$$

$$|(01)\rangle_2^k = (1 - P_{01} + P_{10} - P_{11})|C^k\rangle \quad (17)$$

$$|(10)\rangle_3^k = (1 + P_{01} - P_{10} - P_{11})|C^k\rangle \quad (18)$$

$$|(11)\rangle_4^k = (1 - P_{01} - P_{10} + P_{11})|C^k\rangle \quad (19)$$

(in a more general case this expression can be derived directly from the Hadamard transformation), we can write the decohered state (15) as

$$\sum_{\alpha\beta} A_\alpha P_\beta |C^k\rangle |R_{\alpha\beta}\rangle, \quad (20)$$

where  $\text{wt}(\text{supp}[\alpha] \cup \text{supp}[\beta]) \leq 2$  and  $|R_{\alpha\beta}\rangle$  is the state of the channel/environment which depends on  $\alpha$  and  $\beta$  but, nota bene, not on  $k$ . More precisely,  $|R_{\alpha\beta}\rangle$  can be written as

$$|R_{\alpha\beta}\rangle = \sum_{\gamma} (-1)^{\gamma \cdot \beta} |a_{\gamma, \gamma+\alpha}\rangle \quad (21)$$

where  $\gamma$  can take the binary values 00, 01, 10, 11. An arbitrary encoded state i.e. a superposition of code-vectors  $|C^k\rangle$  of the form

$$|\psi\rangle = \sum_{k=1}^{2^l} c_k |C^k\rangle, \quad (22)$$

evolves under dissipation from the state  $|\psi\rangle |a\rangle$  to

$$\sum_{\alpha\beta} A_\alpha P_\beta \sum_k c_k |C^k\rangle |R_{\alpha\beta}\rangle. \quad (23)$$

Now projections on orthogonal subspaces  $H_{\alpha\beta}$  spanned by  $\{A_\alpha P_\beta |C^k\rangle, k = 1, 2^l\}$  are performed. The results of the projections identify the error locations  $\bar{\alpha}$  and  $\bar{\beta}$  and the appropriate ‘state restoring’ transformation  $P_{\bar{\beta}} A_{\bar{\alpha}}$  is applied. We can see from Eq. (23) that the state after corrections is of the form

$\sum_k c_k |C^k\rangle |R\rangle$ , i.e. the  $n$  qubits system is completely disentangled from the channel/environment. The generalisation to the  $t > 2$  case is straightforward.

Thus we have shown that by a suitable choice of the encoding vectors  $|C^k\rangle$ , which satisfy condition (13), and with amplitude and phase corrections we can increase the probability of an error-free communication in a noisy quantum channel. Let us mention in passing that searching for error locations  $\bar{\alpha}$  and  $\bar{\beta}$  does not have to involve projections on  $H_{\alpha\beta}$  for all allowed values  $\alpha$  and  $\beta$ . This search can be made efficient by starting with projections on subspaces which are unions of several  $H_{\alpha\beta}$  and by subsequent divisions and projections on smaller subspaces.

Quantum encoding requires  $n - l$  auxiliary qubits as an input to the encoder. We will now establish bounds on  $n$ , i.e. number of qubits needed to encode any state of  $l$  qubits. According to what we have shown above, up to  $t$  entanglement-induced errors can be corrected if we can combine two distinct procedures which can correct up to  $t$  amplitude and phase errors. Amplitude and phase errors correspond respectively to operations  $\sigma_x$  and  $\sigma_z$  performed on selected qubits; the two operations performed on the same qubit can be viewed as the third type of error corresponding to operation  $\sigma_y$ . In order to be able to establish the location and the type of errors we require that all the  $2^l$  code-vectors  $|C^k\rangle$  and all the states that are obtained by applying up to  $t$  amplitude and/or phase transformations are mutually orthogonal. The total number of orthogonal states must be smaller than  $2^n$  which is the dimension of the Hilbert space of  $n$  qubits. Thus if we have  $i$  errors of the three types  $\sigma_x$ ,  $\sigma_y$ , and  $\sigma_z$  in an  $n$ -qubits state there are  $3^i \binom{n}{i}$  different ways in which they can occur and the argument based on counting orthogonal states reduces to

$$2^l \sum_{i=0}^t 3^i \binom{n}{i} \leq 2^n. \quad (24)$$

Eq. (24) is the quantum version of the Hamming bound for classical error-correcting codes [2]; given  $l$  and  $t$  it provides a lower bound on  $n$ . The quantum version of the classical Gilbert-Varshamov bound [2] can be also obtained:

$$2^l \sum_{i=0}^{2t} 3^i \binom{n}{i} \geq 2^n. \quad (25)$$

This expression can be proved from the observation that in the  $2^n$  dimensional Hilbert space with a maximum number of code-vectors  $|C^k\rangle$  any vector which is orthogonal to  $|C^k\rangle$  (for any  $k$ ) can be reached by applying up to  $2t$  error operations of  $\sigma_x$ ,  $\sigma_y$ , and  $\sigma_z$  type to any of the  $2^l$  code-vectors. Clearly all vectors which cannot be reached in the  $2t$  operations can be added to the code-vectors  $|C^k\rangle$  as all the vectors into which they can be transformed by applying up to  $t$  amplitude and/or phase transformations are orthogonal to all the others. This situation cannot happen because we have assumed that the number of code-vectors is maximal. Thus the number of orthogonal vectors that can be obtained by performing up to  $2t$  transformations on the code-vectors must be at least equal to the dimension of the encoding Hilbert space.

It follows from Eq.(24) that protecting one qubit against one error ( $l = 1$ ,  $t = 1$ ) requires at least 5 qubits and, according to Eq. (25), this can be achieved with less than 10 qubits. Indeed, explicit constructions of quantum codes for  $n = 9$ ,  $n = 7$  and  $n = 5$  are known [3, 4, 5].

The asymptotic form of the quantum Hamming bound (24) in the limit of large  $n$  is given by

$$\frac{l}{n} \leq 1 - \frac{t}{n} \log_2 3 - H\left(\frac{t}{n}\right), \quad (26)$$

The corresponding asymptotic form for the quantum Gilbert-Varshamov bound (25) is

$$\frac{l}{n} \geq 1 - \frac{2t}{n} \log_2 3 - H\left(\frac{2t}{n}\right), \quad (27)$$

where  $H$  is the entropy function  $H(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ .

Our general requirements for quantum error correcting codes (Eq. (13)) apply to a variety of codes including quantum codes based on classical error correcting schemes (c.f. constructions proposed by Calderbank and Shor [6], and by Steane [4, 7]). Like in the classical case there is probably no systematic way to construct good quantum error correcting codes but we hope that criterium (13) will make future heuristic approaches easier.

Although we have presented the unitary encodings and the decoding projections in a fairly abstract way they can be implemented in practice as a sequence of quantum controlled-NOT logic gates [8]. For experimental purposes gates that operate directly on carriers of information, such as recently

proposed implementation of the controlled-NOT operating directly on polarised photons [9], seem to be very well suited for quantum communication. Other possible applications of quantum error correction may involve improving some high precision measurements e.g. frequency standards based on trapped ions. Properly encoded quantum states of ions will be more robust to dephasing mechanisms such as, for example, collisions with the buffer gas and may have much longer lifetime. Finally let us also point out that the encoding described in this paper applies both to pure and mixed states. In particular it can be used in distribution of entangled particles because it allows to encode (and therefore protect against errors) each particle separately without destroying the entanglement. It may also lead to better quantum cryptographic protocols [10].

## References

- [1] W.H. Zurek, Phys. Today, October p. 36 (1991); connections between phase fluctuations and decoherence in quantum computers are also discussed in: G.M. Palma, K.-A. Suominen, and A. Ekert, Proc. R. Soc. Lond. A **452**, 567 (1996).
- [2] F.J. MacWilliams and N.J.A. Sloane, *The theory of error correcting codes*, Amsterdam: North Holland (1977).
- [3] P. Shor, Phys. Rev. A **52**, R2493 (1995).
- [4] A. Steane, *Multiple particle interference and quantum error correction*, submitted to Proc. R. Soc. Lond. A.
- [5] C. Bennet, D. DiVincenzo, J. Smolin and W. Wootters, unpublished.
- [6] A.R. Calderbank and P.W. Shor, *Good quantum error-correcting codes exist*, submitted to Phys. Rev. A.
- [7] For example, the code-vectors can be constructed from selected codewords  $\{v_i\}$  as  $|C^k\rangle = \sum_i |v_i^k\rangle$ . Requirement (11) implies that for any  $\alpha$  and  $\alpha'$  (both of weight less than  $t$ )  $v_i^k + \alpha + \alpha' \neq v_j^l$ . This means that the selected codewords must be separated at least by the Hamming distance  $2t + 1$ . Requirement (12) implies that  $\sum_i (-1)^{v_i^k \cdot (\beta + \beta')} = \delta_{\beta\beta'}$  for any  $k$ ,



$\beta$  and  $\beta'$  ( $\text{wt}(\beta), \text{wt}(\beta') \leq t$ ). If for a given  $k$  the codewords  $\{v_i^k\}$  form a linear code  $\mathcal{C}$  then this condition is satisfied when the dual code  $\mathcal{C}^\perp$  has minimum distance  $2t + 1$ .

- [8] R. Feynman, Int. J. Theor. Phys. **21**, 467 (1982); A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).
- [9] Q.A. Turchette, C.J. Hood, W. Lange, H. Mabuchi and H.J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).
- [10] S. Wiesner, *SIGACT News*, **15**, 78 (1983); C. H. Bennett and G. Brassard, in “Proc. IEEE Int. Conference on Computers, Systems and Signal Processing”, IEEE, New York, (1984); A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).